DCI Director of Central Intelligence

COMPUTER SECURITY MANUAL

Prepared for
The Director of
Central Intelligence
by the
Security
Committee

Confidential
4 January 1983

SECURITY POLICY ON INTELLIGENCE INFORMATION IN AUTOMATED SYSTEMS AND NETWORKS

(Effective 4 January 1983) [1]

Pursuant to the provisions of the Director of Central Intelligence Directive (DCID) on the Security Committee, policy is herewith established for the security of classified intelligence information (hereafter referred to as intelligence) [2] processed or stored in automated systems and networks.

1. Applicability

The controls and procedures in these provisions and the attached Computer Security Manual shall be applied by all Intelligence Community agencies. Intelligence Community agencies which release or provide intelligence to contractors, consultants or other government departments or agencies shall ensure beforehand that the intended recipients agree to follow these controls and provisions in their own processing or storing of intelligence in automated systems and networks.

Senior Officials of the Intelligence Community (SOICs) [3] shall ensure that the controls and procedures in these provisions and the attached manual are incorporated in regulations on this subject issued by Intelligence Community agencies.

The diversity and complexity of automated systems and networks in use by, or already designed for future placement in, the Community may not permit full compliance with these controls and procedures. Accordingly, SOICs are granted discretion on the application to their automated systems and networks of the exceptions stated in these provisions, consistent with the responsibility of SOICs for the protection of all intelligence in their custody.

2. Responsibilities

Each SOIC or his designee is responsible for ensuring compliance by his/her respective organization, and any other organization for which he/she has security responsibility, with these provisions and the attached Computer Security Manual. However, only an SOIC may accredit an automated system or network for operation in the Compartmented Mode.

3. Policy

SOICs shall establish and maintain within their agencies formal computer security programs to ensure that intelligence processed or stored by automated systems

---

[1] These provisions supersede those in DCID 1/16, effective 6 June 1982. They derive from and have the force of the DCID on the Security Committee, effective 15 July 1982.

[2] For purposes of this policy statement, classified intelligence information ("intelligence") means foreign intelligence, and foreign counterintelligence involving sensitive intelligence sources or methods, that has been classified pursuant to Executive Order 12356 (or successor Order). "Foreign intelligence" and "counterintelligence" have the meanings assigned them in Executive Order 12333. "Intelligence," as used herein, also includes Sensitive Compartmented Information (SCI) as defined in the DCI Security Policy Manual for SCI Control Systems, effective 28 June 1982 (or successor manual).

[3] Senior Officials of the Intelligence Community (SOICs), for purposes of these provisions, are the heads of organizations within the Intelligence Community, as defined by Executive Order 12333, or their designated representatives for intelligence matters.

and networks is adequately protected. The minimum security requirements for the allowed modes of operation of automated systems and networks are contained in the attached Computer Security Manual. Additional computer security measures may be established if deemed appropriate. Automated systems or networks shared with foreign governments shall be addressed on a case-by-case basis by the SOIC(s) involved in consultation with the DCI or his designee for this purpose.

4. Exceptions

a. These provisions do not apply to automated systems or networks used exclusively for telecommunications services. Security policy on such services is provided by the National Communications Security Committee.

b. SOICs or their designees may temporarily exempt specific automated systems or networks under their jurisdiction from complete compliance with these provisions and the attached manual when compliance would significantly impair the execution of their missions. Chapter III of the attached manual governs when the system being exempted is part of an automated network as defined therein. An exemption may be granted only when the SOIC or his/her designee is assured that the other security measures in effect will adequately protect the intelligence being processed. The SOIC or his/her designee granting an exception shall strive for the earliest feasible attainment of complete compliance. No exception shall be granted which would allow personnel with less than a TOP SECRET clearance based on a background investigation to access an automated system or network which contains SCI.

c. Nothing in these provisions or the attached Computer Security Manual supersedes requirements under the Atomic Energy Act of 1954, as amended (Section II, Public Law 585), on the control, use, and dissemination of Restricted Data or Formerly Restricted Data, or requirements regarding Communications Security (COMSEC) related material as established by or under existing statutes, directives, or Presidential policy.

Attachment:
DCI Computer Security Manual

Approved For Release 2005/12/01 : CIA-RDP96B01172R000600040006-7

COMPUTER SECURITY MANUAL

(Attachment to "Security Policy on Intelligence Information in Automated Systems and Networks")

Approved For Release 2005/12/01 : CIA-RDP96B01172R000600040006-7

Table of Contents

CHAPTER I

Introduction

I.1. Director of Central Intelligence security policy requires Intelligence Community agencies and all other United States Government departments and agencies processing and/or storing intelligence information in ADP systems and networks to establish and maintain a formal ADP security program to ensure adequate protection of intelligence information. This Manual is promulgated to establish the minimum security requirements for the allowed operating modes of an ADP system or network as defined in Chapters II and III. ADP security programs shall be based on these programs.

I.2. All ADP systems and networks not otherwise exempted pursuant to DCI Security Policy on Intelligence Information in Automated Systems and Networks, which process and/or store intelligence information, must meet the requirements prescribed in Chapters II and III of this Manual. Accreditation, as prescribed herein, is required for the operation of each ADP system and network. The accreditation is contingent upon the results of a recurring review, testing, and favorable evaluation of employed security features. These security features shall include hardware/software features, operating procedures, accountability procedures, access controls, management constraints, physical structures, and appropriate communications security (COMSEC) measures to provide minimum security protection for intelligence information processed and/or stored by the ADP system or network.

I.3. An Information System Security Officer (ISSO) shall be appointed for each ADP system processing and/or storing intelligence information. An ISSO may serve for more than one system. Duties and responsibilities of the ISSO are specified in Chapters II and III.

I.4. The SOIC or his designee responsible for the management of an ADP network shall appoint a Network Security Officer (NSO). Duties and responsibilities of the NSO are specified in Chapter III of this Manual.

Next 9 Page(s) In Document Exempt

Approved For Release 2005/12/01 : CIA-RDP96B01172R000600040006-7

GLOSSARY

The following definitions apply to the terms used in the Computer Security Manual.

Access. The ability and the means to approach, communicate with (input to or receive output from), or otherwise make use of any material or component in an ADP system or network.

Accreditation. A formal declaration by the responsible SOIC, or his designee, as appropriate, that the ADP system or network provides an acceptable level of protection for processing and/or storing intelligence information. An accreditation should state the operating mode and other parameters peculiar to the ADP system or network being accredited.

ADP System. The central computer facility and any remote processors, terminals, or other input/output/storage devices connected to it by communications links. Generally, all of the components of an ADP system will be under the authority of one SOIC or his designee.

Authentication. A positive identification, with a degree of certainty sufficient for permitting certain rights or privileges to the person or thing positively identified.

Central Computer Facility. One or more computers with their peripherals and storage units, central processing units, and communications equipment in a single controlled area. This does not include remote computer facilities, peripheral devices, or terminals which are located outside the single controlled area even though they are connected to the central computer facility by approved communication links.

Escort. Duly designated personnel who have appropriate clearances and access approvals for the material contained in the ADP system and are sufficiently knowledgeable to understand the security implications and to control the activities and access of the individual being escorted.

Front-end Processor. A computer associated with a host computer that performs preprocessing functions. It may perform line control, message handling, code conversion, error control, data control, data management, terminal handling, etc. (See Manual, Chapter III, Figure 1.)

Operating System (O/S). An integrated collection of service routines for supervising the sequencing and processing of programs by a computer. Operating systems control the allocation of resources to users and their programs and play a central role in assuring the secure operation of a computer system. Operating systems may perform input/output, accounting, resource allocation, compilation, storage assignment tasks, and other system-related functions.

Processing and/or Storing. All inclusive term used to include in addition to processing and storing such functions as manipulating, deleting, modifying, editing, outputting, etc.

Sensitive Compartmented Information (SCI). All information and materials requiring special Community controls indicating restricted handling within present and future Community intelligence collection programs and their end products. These special Community controls are formal systems of restricted access established to protect the sensitive aspects of sources and methods and analytical procedures of foreign intelligence programs. The term does not include Restricted Data as defined in Section II, Public Law 585, Atomic Energy Act of 1954, as amended.

Approved For Release 2005/12/01 : CIA-RDP96B01172R000600040006-7